AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) In a computerized network environment including two or more computer systems sending messages through a network communication protocol, a method of receiving secure messages using custom security tokens, the method comprising:

an act of receiving a message, the message comprising a serialized portion and a non serialized portion, wherein the serialized portion is serialized based on a key that can be accessed at a key provider, wherein the message comprises key identity information for the key, and wherein the non-serialized portion comprises destination information, such that intermediate computer systems that relay the message to a receiving computer system do not need to deserialize portions of the message to identify an intended recipient of the message;

an act of deserializing at least a portion of the serialized portion, wherein the serialized portion that is deserialized comprises one or more security tokens created using one or more value types;

an act of identifying the one or more security tokens in the received message that has at least a portion that has been encrypted using the one or more security tokens, and a value type corresponding with each identified security token, ;

an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access, wherein the stored value type comprises a custom program class including a collection of executable instructions for data handling, including instructions that tell a computer system how to read data associated with a specific security token that was created using the value type;

an act of receiving data from the at least one identified security token into the stored value type that has been matched; and

an act of decrypting an encrypted portion of the received message and accessing the received message based at least in part on the raw data received from the at least one identified security token.

2. (Original) The method as recited in claim 1, wherein the received message includes one or more digital signatures, the method further comprising an act of authenticating at least one of the one or more digital signatures.

3. (Original) The method as recited in claim 1, further comprising an act of receiving a message from a sending computer system, the message including an encrypted portion and one or more security tokens.

4. (Cancelled)

5. (Cancelled)

6. (Previously Presented) The method as recited in claim 1, wherein the identified corresponding value type is a custom value type created by the sending computer system or the receiving computer system, and that the receiving and sending computer system can access.

7. (Original) The method as recited in claim 1, further comprising an act of updating one or more properties of the stored security token that is accessible by the receiving computer system with one or more of the identification information and the custom property.

8. (Original) The method as recited in claim 7, further comprising an act of creating a security key when updating the one or more properties of the stored security token.

9. (Original) The method as recited in claim 1, wherein the identified at least one security token is serialized in the received message based on a private key that is shared between the sending and receiving computer system.

10. (Cancelled)

11. (Original) The method as recited in claim 1, wherein the one or more security tokens are found in a security header portion of the message.

12. (Original) The method as recited in claim 11, wherein, prior to receiving the message, the at least one identified token is serialized into the security header portion of the message by transforming the at least one identified security token into base 64 encoded data.

13. (Original) The method as recited in claim 12, wherein deserializing comprises an act of converting data from the identified at least one token from base 64 encoding to a byte array.

14. (Previously Presented) In a computerized network environment including two or more computer systems sending messages through a network communication protocol, a method of receiving secure messages using custom security tokens, the method comprising:

an act of at a receiving computer system identifying one or more security tokens in a received message, from a sending computer system, that has at least a portion that has been encrypted using the one or more security tokens, and a value type corresponding with each identified security token, wherein the identified value type is a custom program class that only the receiving computer system and the sending computer system can access, wherein the stored value type comprises a custom program class including a collection of executable instructions for data handling, including instructions that tell a computer system how to read data associated with a specific security token that was created using the value type;

an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access; and

an act of receiving data from the at least one identified security token into the stored value type that has been matched, wherein the raw data includes one or more of identification information, and a custom property; and

an act of decrypting an encrypted portion of the received message using the stored value type based at least in part on the raw data received from the at least one identified security token.

15-16 (Cancelled)

17. (Previously Presented) In a computerized network environment including two or more computer systems sending messages through a network communication protocol, a method of sending secure messages using custom security tokens, the method comprising:

an act of a sending computer system generating one or more security tokens using one or more corresponding value types, wherein the one or more corresponding value type comprise custom program classes including collections of executable instructions for data handling, including instructions that tell a computer system how to read data associated with a specific security token that was created using a specific value type, each token including token data that includes a custom property, wherein the custom property defines one or more of time of day, geographic location, limitations on message access, or limitations on device access;

an act of encrypting a portion of a message using at least one of the one or more generated security tokens;

an act of inserting the at least one generated security token in an outbound token collection; and

an act of converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system.

18. (Original) The method as recited in claim 17, further comprising an act of including one or more digital signatures in the message, wherein the one or more digital signatures are authenticated prior to decrypting the encrypted portion of the message.

19. (Previously Presented) The method as recited in claim 17, further comprising an act of including private key information in the message, such that the receiving computer system can access the key from a key provider based on the key information.

20. (Original) The method as recited in claim 17, wherein the act of converting the token data comprises serializing the token data into base 64 encoding.

21. (Original) The method as recited in claim 17, wherein the at least one generated security token is a custom security token created using a custom value type, and wherein the custom value type is accessible by both the sending and receiving computer systems.

22. (Original) The method as recited in claim 17, further comprising an act of creating a signature or encryption function based on the included one or more of a custom property, a signature, and an encryption level in the created binary token.

23. (Original) The method as recited in claim 17, further comprising an act of including a program language value corresponding with each token that is included in the outbound token collection.

24. (Original) The method as recited in claim 23, wherein the program language value is a Common Language Runtime value.

25. (Cancelled)

26. (Previously Presented) The method as recited in claim 17, further comprising an act of assigning the markup language representation of the at least one generated security token a global unique identifier.

27. (Original) The method as recited in claim 26, wherein the outbound token collection is a hash table that is keyed by the global unique identifier of the at least one generated security token.

28. (Original) The method as recited in claim 27, wherein the global unique identifier is inserted into a signature or encryption portion of the message.

29.   (Previously Presented) In a computerized network environment including two or more computer systems sending messages through a network communication protocol, a method of sending secure messages using custom security tokens, the method comprising:

an act of a sending computer system generating one or more security tokens using one or more corresponding value types, wherein the one or more corresponding value type comprise custom program classes including collections of executable instructions for data handling, including instructions that tell a computer system how to read data associated with a specific security token that was created using a specific value type, each token including token data that includes one or more of a custom property, a signature, and an encryption level;

an act of encrypting a portion of a message using at least one of the one or more generated security tokens;

an act of inserting the at least one generated security token in an outbound token collection; and

an act of converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system.

30-31 (Cancelled)

32.   (Previously Presented) The method as recited in claim 14, wherein deserializing comprises an act of converting data from the identified at least one token from base 64 encoding to a byte array.

33.   (Previously Presented) The method as recited in claim 29, wherein the program language value is a Common Language Runtime value.

34. (Previously Presented) The method as recited in claim 1, wherein the one or more security tokens are represented in the message by a markup language identifier, and wherein the at least one identified security token is identified by the markup language identifier.

35. (Previously Presented) The method as recited in claim 17, wherein the act of inserting the at least one generated security token in an outbound token collection further comprises:

an act of identifying a markup language representation of the at least one generated security token, and

an act of placing the markup language representation of the at least one generated security token in the outbound token collection.

36. (Previously Presented) The method as recited in claim 1, wherein the value type comprises compiled instructions.